1. Czy podmiot ma licencję na obsługę e-zamówień publicznych zgodną z projektem „e-zamówienia)?Jeśli nie to czy w budżecie na roku 2022 i kolejne planujecie środki na ten cel?

Odp. TAK

2. Czy są planowane przetargi na artykuły biurowe w roku 2022 i w kolejnych latach?

Odp. NIE

3. *W związku z §20 pkt. 12 lit. a Rozporządzenia dt. Krajowych Ram Interoperacyjności -*

   „ zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: dbałości o aktualizację oprogramowania,(...) "

   - wnosimy o udzielnie informacji publicznej w przedmiocie - szacunkowej ilości oprogramowania - użytkowanego w podmiocie i nieposiadającego obecnie wsparcia producenta - inter alia: Windows XP, Windows 7, Windows Vista, etc. Dodatkowo wnosimy o wyszczególnienie i podanie wszystkich narzędzi oraz systemów informatycznych zakupionych z środków publicznych.

   Odp. zapewniony jest dostęp bezpieczeństwa w systemach teleinformatycznych - oprogramowanie jest aktualizowane na bieżąco;

4. Proszę o ocenę poszczególnych systemów informatycznych(pkt.3) w skali od 1 do 10 (0-najniższa ocena, 10 -najwyższa).

Odp. ocena - 7 pkt.

5. Czy podmiot korzysta lub korzystała w latach ubiegłych z usług firm zewnętrznych np. w zakresie przetargów, rekrutacji bezpieczeństwa informacji ,a jeżeli tak to proszę o podanie: dat obowiązywania umowy, wysokości wynagrodzenia, przedłożenie skanu umowy w formie elektronicznej

Odp. nie korzystamy z usług firm zewnętrznych w zakresie przetargów.

6. Proszę o ocenę poszczególnych firm zewnętrznych (pkt.5) w skali od 1 do 10 (0-najniższa ocena, 10 -najwyższa).

Odp. nie dotyczy

7. Wnosimy o przesłanie kopii treści instrukcji kancelaryjnej

Odp: Posiadamy instrukcję kancelaryjną - zarządzenie wewnętrzne

Lp.	Zagadnienie	*Tak*	Nie	Uwagi

Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.				
1.	Czy prowadzona jest ewidencja:			
	a) sprzętu informatycznego w ramach ewidencji majątkowej?CZY IOD KONTROLUJĘ EWIDENCJĘ	tak		wyznaczona osoba przez administratora
	b) oprogramowania (np. licencje)? IOD KONTROLUJĘ EWIDENCJĘ	tak		wyznaczona osoba przez administratora
	c) umów serwisowych?	tak		-
2.	Czy przypisano konkretnym osobom obowiązki w zakresie prowadzenia powyższych ewidencji - w tym oprogramowania i nośników oprogramowania? Jeśli TAK proszę o przedłożenie dokumentu. CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W	tak		audyt przeprowadzany jest raz w roku w ustalonym z administratorem terminie
3.	Czy posiadam zinwentaryzowany sprzęt / oprogramowanie wraz z określeniem ważności danego komponentu dla całej jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE*	tak		wyznaczona osoba przez administratora

	SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W			
4.	Czy pracownicy mogą używać swojego sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych? IOD KONTROLUJĘ EWIDENCJĘ		nie	
5.	Czy pracownicy mogą podłączać swój sprzęt (laptopy, telefony, tablety) do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		nie	zgodnie z Instrukcją zarzadzania RODO
6.	Czy zapisuję każdy fakt podłączenia zewnętrznego sprzętu do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			nie dotyczy
7.	Czy monitoruję podłączenia ewentualnych nieautoryzowanych punktów bezprzewodowych do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			nie dotyczy
Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.				
1.	Czy znam najistotniejsze zagrożenia dla zinwentaryzowanych systemów IT?	tak		

	Jeśli TAK proszę o ich wskazanie .			
2.	Czy wiem, które systemy są krytyczne dla działania jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	tak		
3.	Czy mam pewność, że każdy krytyczny system jestem w stanie odtworzyć z kopii zapasowych w odpowiednim czasie? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	tak		
4.	Czy mam opracowane plany działania w momencie naruszenia bezpieczeństwa IT w mojej organizacji (np. procedury reagowania na incydenty IT)?	tak		
5.	Czy znam potencjalne zagrożenia dla systemów, które znajdują się w mojej infrastrukturze lub w infrastrukturze zewnętrznej (outsourcing)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	tak		
Podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji wraz z bezzwłoczną zmianą uprawnień, w przypadku zmiany zadań.				
1.	Czy wskazana/e jest/są w jednostce osoba/y odpowiedzialna/e za bezpieczeństwo IT w	tak		

	jednostce? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W* Jeśli TAK proszę o przedłożenie dokumentu.			
2.	Czy osoby te posiadają stosowne kompetencje? Jeśli TAK proszę o potwierdzenie tego faktu.	tak		
3.	Czy wszyscy pracownicy zaangażowani w proces przetwarzania informacji posiadają pisemne uprawnienia?	tak		
4.	Czy uprawnienia, o których mowa w pkt 3 uprawniają jedynie do przetwarzania informacji w stopniu adekwatnym do realizowanych zadań? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	tak		
5.	Czy identyfikatory i hasła nadawane są po uprzednim pisemnym złożeniu wniosku?			zgodnie z procedurą nadawanie haseł
6.	Czy na bieżąco aktualizowane są uprawnienia do dostępu (np. w momencie zmiany zakresu obowiązków)? *CZY IOD W TYM ZAKRESIE*	tak		

	PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W			
7.	Czy prowadzona jest formalna listę zadań /obowiązków /uprawnień takich osób? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	tak		
Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.				
	Należy zaznaczyć stosowane w jednostce rozwiązania.			
1.	Bieżące czynności monitorowania dostępu w tym logi (serwery, systemy, urządzenia sieciowe).			nie dotyczy
2.	Podstawowe elementy ochrony przed nieautoryzowanymi działaniami związanymi z przetwarzaniem informacji:			
a.	ochrona sieci na poziomie portów LAN	tak		
b.	BIOS		nie	
c.	centralny system kontroli dostępu logicznego do pojedynczych komputerowych stanowisk pracy, serwerów i zasobów sieci - na poziomie domeny Windows		nie	
d.	niezależne od domenowych systemy kontroli dostępu logicznego do kluczowych systemów informatycznych; *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE*		nie	

	Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W			
e.	system ochrony zewnętrznej klasy firewall	tak		
f.	system ochrony zewnętrznego dostępu logicznego (urządzanie sieciowe-serwer VPN); – zabezpieczenie kodem PIN dostępu do wydruków;		nie	
g.	stosowanie tokenów z hasłami jednorazowymi		nie	

Podstawowe zasady

gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE PRACĘ NA ODLEGŁOŚĆ CZY TYLKO PRZEDSTAWIA DOKUMENTY.*

1.	Czy wprowadzono regulacje wewnętrzne jednostki w zakresie zdalnego dostępu do zasobów informatycznych/pracy na odległość? *Jeśli TAK proszę o przedłożenie dokumentu* .	tak		regulamin pracy zdalnej
2.	Czy w umowach zawieranych z podmiotami zewnętrznymi określono zakres i tryb dostępu do własnych zasobów IT?	tak		

	Jeśli TAK proszę o udokumentowanie.			
3.	Czy w pracy na odległość stosuję bezpieczne metody połączenia?	tak		
4.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, posiadają aktualne oprogramowanie antywirusowe/są w pełni zaktualizowane?	tak		
5.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, są chronione przed utratą danych (np. w wyniku kradzieży)? Jeśli TAK proszę wskazać, w jaki sposób.	tak		kopie danych
Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*				
1.	Czy jednostka posiada zapisy gwarantujące odpowiedni poziom bezpieczeństwa IT w umowach zawieranych z dostawcami sprzętu/ oprogramowania? Jeśli TAK proszę o udokumentowanie.	tak		
2.	Czy posiadam krytyczne systemy, dla których nie ma zapisów umownych dotyczących bezpieczeństwa (np. zapewnienie możliwości			nie dotyczy

	wgrania aktualizacji komponentów, na których bazuje dany system)?			
Zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. CZY IOD PRZEPROWADZIŁ ANALIZĘ RYZYKA I OCENĘ SKUTKÓW DLA PRZETWARZANIA DANYCH W URZĄDZENIACH MOBILNYCH?*				
1.	Czy obowiązują odpowiednie regulacje dotyczące zapisu danych na nośnikach przenośnych? Jeśli TAK proszę o przedłożenie.	tak		
2.	Czy posiadam mechanizmy uniemożliwiające dostęp do danych na urządzeniu mobilnym po jego utraceniu (np. pin/szyfrowanie przestrzeni dyskowej na urządzeniu)?			nie dotyczy
3.	Czy istniej możliwość zdalnego, trwałego usunięcia danych z tego typu urządzenia?			nie dotyczy
4.	Czy kontroluję to, co użytkownicy mogą realizować na urządzeniach mobilnych (np. uruchamianie dowolnych aplikacji)?			nie dotyczy
5.	Czy mam zapewnione bezpieczne połączenie urządzeń mobilnych z moją infrastrukturą (np. tylko protokoły szyfrowane)?			nie dotyczy
6.	Czy pracownicy mogą podłączać swoje urządzenia mobilne do mojej infrastruktury IT?		nie	
Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE*				

SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. ANALIZA RYZYKA W/W.				
1.	Czy realizuję bieżące aktualizacje zarówno na stacjach PC (system operacyjny / java / adobe reader / flash itp.), jak i serwerach?	tak		
2.	Czy aktualizuję oprogramowanie firmware na urządzeniach sieciowych – szczególnie tych, które mają bezpośredni styk z Internetem?			nie dotyczy
3.	Czy posiadam aktualne sygnatury dla systemu antywirusowego?	tak		
4.	Czy mam przygotowaną procedurę odtworzenia danej stacji roboczej / serwera po wykryciu na nim wirusa?	tak		
5.	Czy mam informacje o systemach, dla których aktualizacja nie powiodła się?		nie	
6.	Czy wiem, które systemy IT są krytyczne dla prawidłowego działania jednostki?	tak		
7.	Czy zapewniono ciągłość działania w przypadku wystąpienia awarii ww. systemów?	tak		
8.	Czy użytkownicy sieci przesyłają wrażliwe informacje w formie jawnej (np. za pośrednictwem e-mail lub przenosząc na pendrive / telefonie)?	tak		emaile szyfrowane polaczenie
9.	Czy obowiązuje w jednostce instrukcja reagowania na incydenty bezpieczeństwa IT?	tak		
10.	Czy wiem, z jakimi innymi wymaganiami prawnymi muszą być zgodne użytkowane systemy?	tak		

11	Czy zapewniam odpowiednio bezpieczny dostęp do poczty elektronicznej (dostęp tylko szyfrowany)?	tak		
12.	Czy umożliwiony jest zdalny dostęp do poczty elektronicznej?	tak		
13.	Czy dostęp do Internetu w jednostce jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp)?		nie	
14.	Czy w odpowiedni sposób zapewnia się ochronę przed fizyczną ingerencją w infrastrukturę IT (np.: odpowiednie zabezpieczenia serwerowni, okablowania)	tak		
Zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.				
1.	Czy istnieją w jednostce procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?	tak		
2.	Czy okresowo testuje się procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?	tak		podczas corocznego audytu

WNOSIMY DODATKOWO O UDZIELENIE INFORMACJI PUBLICZNEJ?

1. Kto (imię, nazwisko, stanowisko). sprawował nadzór nad WYZNACZENIEM IOD, wyboru IOD w zakresie rozdysponowania środków publicznych na rzecz zewnętrznego IOD?

Ad1. Karol Choynowski – dyrektor szkoły

2.Wnosimy o podanie danych sekretarza, kierowników jednostek organizacyjnych jego wykształcenia, przebiegu zatrudnienia.

Ad. 2 Nie posiadamy takich informacji.

Na pytania z wniosku II udzielono już wcześniej odpowiedzi na Państwa maila z dnia 13.07. 2022 roku. Pytania i odpowiedzi zamieszczono na stronie internetowej szkoły w zakładce BIP – informacja publiczna.

Na pytania z wniosku V i VII, VIII, IX i X udzielono już o wcześniej odpowiedzi na Państwa maila z dnia 13.07. 2022 roku. Pytania i odpowiedzi zamieszczono na stronie internetowej szkoły w zakładce BIP – informacja publiczna.

W dniu 19 września 2022 zostały umieszczone na stronie szkolnej wszystkie maile od Państwa i odpowiedzi na nie.